

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-037590

(43)Date of publication of application : 07.02.2003

(51)Int.Cl.

H04L 9/14

G06F 12/14

(21)Application number : 2001-380390

(71)Applicant : SHARP CORP

(22)Date of filing : 13.12.2001

(72)Inventor : EZURE KATSUYOSHI

(30)Priority

Priority number : 2001149824

Priority date : 18.05.2001

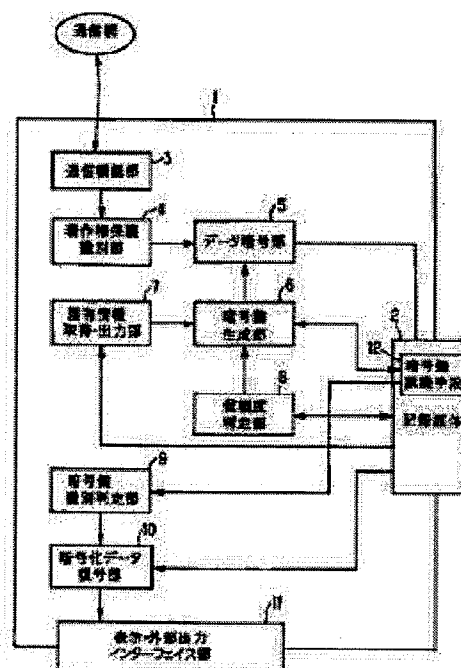
Priority country : JP

(54) INFORMATION PROCESSOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information processor with an encryption device, which can improve protection of the copyright to the received data and can deal with the life of a recording medium suitably.

SOLUTION: This processor is provided with a copyright protection identification part 4 to identify whether the received data is the data protected by the copyright or not and a reliability decision part 8 to decide the reliability of a recording medium 2. A encryption key is formed in the encryption key formation part 6 based on the prescribed information of the recording medium 2 in the case the reliability of the recording medium 2 is high in the reliability decision part 8 when the data identified that it is protected by the copyright in the copyright protection identification part 4 is enciphered. On the other hand, when it is determined that the reliability of the recording medium 2 is low, the encryption key is formed based on the prescribed information of the information processor 1.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-37590
(P2003-37590A)

(43) 公開日 平成15年2月7日 (2003. 2. 7)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L 9/14		G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
G 0 6 F 12/14	3 2 0		3 2 0 F 5 J 1 0 4
		H 0 4 L 9/00	6 4 1

審査請求 未請求 請求項の数5 O L (全 7 頁)

(21) 出願番号 特願2001-380390(P2001-380390)
(22) 出願日 平成13年12月13日 (2001. 12. 13)
(31) 優先権主張番号 特願2001-149824(P2001-149824)
(32) 優先日 平成13年5月18日 (2001. 5. 18)
(33) 優先権主張国 日本 (J P)

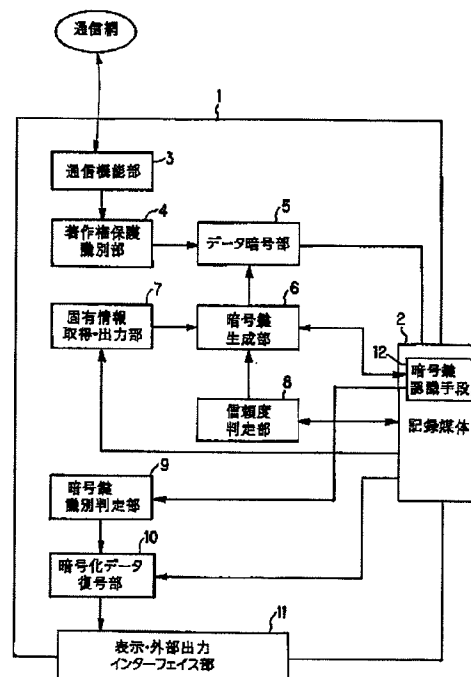
(71) 出願人 000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72) 発明者 江連 克佳
大阪府大阪市阿倍野区長池町22番22号 シ
ャープ株式会社内
(74) 代理人 100112335
弁理士 藤本 英介
Fターム(参考) 5B017 AA06 BA07
5J104 AA01 AA35 AA37 NA02 PA14

(54) 【発明の名称】 情報処理装置

(57) 【要約】

【課題】 受信したデータに対して、その著作権の保護を強化することが可能で、かつ記録媒体の寿命に適切に対応することが可能な暗号化装置を備えた情報処理装置を提供する。

【解決手段】 受信データが著作権により保護されたデータであるか否かを識別するための著作権保護識別部4と、記録媒体2の信頼度を判定するための信頼度判定部8とを備える。著作権保護識別部4において著作権により保護されていると識別されたデータに対して暗号化を行う際に、暗号鍵生成部6では、信頼度判定部8において記録媒体2の信頼度が高いと判定されると、記録媒体2の固有情報に基づいて暗号鍵を生成する。一方、記録媒体2の信頼度が低いと判定されると、当該情報処理装置1の固有情報に基づいて暗号鍵を生成する。



【特許請求の範囲】

【請求項1】 データを受信するための受信手段と、該受信手段により受信した受信データを暗号化するための暗号化手段と、該暗号化手段により暗号化した受信データを交換可能な記録媒体に記録するための記憶手段とを備え、前記記録媒体に記録された受信データを新規な記録媒体に複写可能な情報処理装置において、前記受信データが著作権により保護されたデータであるか否かを識別するための著作権保護識別手段と、前記記録媒体の信頼度を判定するための信頼度判定手段とを備え、前記著作権保護識別手段において著作権により保護されていると識別されたデータに対して、前記暗号化手段により暗号化を行う際に、前記信頼度判定手段において前記記録媒体の信頼度が高いと判定された場合には、前記記録媒体の固有情報に基づいて暗号鍵を生成して暗号化を行うとともに、前記信頼度判定手段において前記記録媒体の信頼度が低いと判定された場合には、当該情報処理装置の固有情報に基づいて暗号鍵を生成して暗号化を行うことにより、著作権を保護することを特徴とする情報処理装置。

【請求項2】 前記記録媒体に記録されたデータに対して用いられている暗号鍵の種類を識別するための暗号鍵識別手段を備えたことを特徴とする請求項1記載の情報処理装置。

【請求項3】 前記記録媒体に対してデータを暗号化して記録する際に、当該記録媒体において前記暗号鍵の種類が混在しないようにすることを特徴とする請求項1記載の情報処理装置。

【請求項4】 データを受信するための受信手段と、該受信手段により受信した受信データが著作権により保護されたデータであるか否かを識別するための著作権保護識別手段と、前記受信データから著作権情報を検出して著作権管理情報を生成するための著作権情報管理手段と、前記受信データを暗号化するための暗号化手段と、該暗号化手段により暗号化した前記受信データを交換可能な記録媒体に記録するための記憶手段とを備え、前記記録媒体に記録された受信データを新規な記録媒体に複写可能な情報処理装置において、当該情報処理装置の固有情報と、前記受信データの著作権情報と、前記著作権情報管理手段で生成した著作権管理情報とに基づいて暗号鍵を生成するための暗号鍵作成手段を備え、前記受信データに対して、前記暗号鍵作成手段で作成した暗号鍵を用いて暗号化を行い暗号化済受信データを生成し、該暗号化済受信データを前記記録媒体に記録することを特徴とする情報処理装置。

【請求項5】 前記受信データの著作権情報が許可した範囲において、前記暗号化済受信データと、該暗号化済受信データを複合化するための暗号鍵を送出し、新規な

記録媒体に複製可能としたことを特徴とする請求項4記載の情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、受信したデータに対して、その著作権の保護を強化することが可能な暗号化装置を備えた情報処理装置に関する。

【0002】

【従来の技術】近年、データ通信が一般化するに伴い、通信機能を有した携帯情報端末装置が普及してきている。これらの携帯情報端末装置には、受信したデータを保存するための記録媒体を備えており、この記録媒体は、例えば、携帯情報端末装置に装着脱可能となった書き換え可能なメモリカードにより構成されている。また、これらの携帯情報端末装置では、受信したデータをメモリカード等の記録媒体に保管する際に暗号化する技術が採用されており、受信データの内容を他人が容易に読むことができないようになっている。

【0003】例えば、特開平9-146457号公報には、情報記録媒体の固有の識別情報を任意の認証番号により暗号化して第1の情報を生成し、この第1の情報を情報記録媒体を取り扱うシステムの所定の情報により暗号化して第2の情報を生成し、この第2の情報の一部を選択して第3の情報を生成し、この第3の情報を情報記録媒体に対する情報の読み取りおよび書き込みを行うための装置の固有の情報により暗号化して情報記録媒体に記録される情報へアクセスするための暗号鍵を生成するようにした技術が開示されている。

【0004】また、特開2000-187935号公報には、通信手段により暗号化されたデジタルデータを受信するための通信手段を有するとともに、データの暗号化を行うための暗号化手段は、記録媒体の識別情報に基づいて生成した暗号鍵によりデータを暗号化するための第1の暗号化部と、記録媒体を取り扱う再生装置の識別情報に基づいて生成した暗号鍵によりデータを暗号化するための第2の暗号化部とを有し、記録媒体が再生装置から着脱可能であると判断した場合には、第1の暗号化部によりデータの暗号化を行なわせ、記録媒体が再生装置から着脱不可であると判断した場合には、第2の暗号化部によりデータの暗号化を行なわせるようにした技術が開示されている。

【0005】また、特開平7-287655号公報には、装置の固有情報を記録媒体に書き込んでおき、この記録媒体が装置に装着された時、装置の固有情報と、記録媒体上に記録済の固有情報を読み出して比較し、固有情報が一致しなかった場合はアクセスを禁止する技術が開示されている。この技術では、固有情報を記録媒体に記録する際に、固有情報を暗号化するようになっている。

【0006】また、特開2000-113586号公報には、記録媒体の保持する固有情報によって暗号化された

鍵と、各情報に特有の識別情報と、前記鍵により暗号化された情報とに基づいて、暗号化された鍵を情報特有の識別情報により特定し、暗号化された情報を複合化して再生する技術が開示されている。

【0007】

【発明が解決しようとする課題】 上述した従来の技術においては、種々の暗号鍵生成方式により生成された暗号鍵を用いて、記録媒体に記録される情報の安全性を高めたり、記録媒体が着脱可能な場合に、暗号鍵の生成方式を制御する方法が採用されている。すなわち、データ秘
10 匿の重要性が増すことにより、その安全性にかかわる暗号鍵の生成および制御はより高度になってゆく。さらに、データを記録するための記録媒体には物理的（電気的）な寿命があることから、データの複写を行い、バックアップしておくことが重要となってくる。

【0008】しかしながら、上述した従来の技術では、着脱可能な記録媒体に対して、当該記録媒体の識別情報に基づいて暗号鍵を制御する方法が採用されている。このため、当該記録媒体のデータを新規な記録媒体に複写
20 すると、元の記録媒体の固有情報と新規な記録媒体の固有情報とが異なることから、複写はできても再生ができなくなってしまうという問題があった。

【0009】また、情報処理装置の固有情報を記録媒体に書き込む方式では、上述した問題を解決することができるものの、データの著作権を無視して複写がなされる可能性が生じるという問題があった。すなわち、データの暗号化に対してある程度の知識を有する者であれば、記録媒体に記録されている暗号化データを一旦復号化して再生し、次に保存する場合に、新規な記録媒体に対し
30 てデータを保存すれば、著作権を無視した複写を行うことができってしまう場合があった。

【0010】また、記録媒体の固有情報に基づいて暗号鍵を生成する方法では、記録媒体自体の寿命或使用環境による寿命（エラーレートの増加）に対応して、記録媒体に記録されたデータを複写することができなかった。すなわち、従来の技術では、ユーザが記録媒体の寿命を知るための手段がないため、ユーザによっては、記録媒体のデータが永久に使用できると思いこんでしまうケースが多々見受けられた。

【0011】また、装置の固有情報と、記録媒体上に記録済の固有情報とを読み出して比較し、固有情報が一致しなかった場合はアクセスを禁止する方法では、記録媒体に記録された情報自体は容易に読み出せるため、別の記録媒体に複製が可能であり、著作権の保護を図ることができなかった。さらに、装置が故障などにより使用不可能となった場合には、それまで記録された情報を他の装置で読み込もうとしても、記録媒体に書き込まれた装置の固有情報が異なるため、読み出しが不可能であった。

【0012】また、記録媒体の保持する固有情報によっ
50

て暗号化された鍵と、各情報に特有の識別情報と、前記鍵により暗号化された情報とに基づいて、暗号化された鍵を情報特有の識別情報により特定し、暗号化された情報を複合化して再生する方法では、各情報に特有の識別情報を利用すれば、各情報を無制限に複製できるので、著作権保持者が望む複製回数の制限が無効となり、結果として著作権保護を図ることができなかった。

【0013】本発明は、上述した事情に鑑み提案されたもので、受信したデータに対して、その著作権の保護を強化することが可能で、かつ記録媒体の寿命に適切に対応することが可能な暗号化装置を備えた情報処理装置を提供することを目的とする。

【0014】

【課題を解決するための手段】 本発明に係る情報処理装置は、データを受信するための受信手段と、該受信手段により受信した受信データを暗号化するための暗号化手段と、該暗号化手段により暗号化した受信データを交換可能な記録媒体に記録するための記憶手段とを備え、前記記録媒体に記録された受信データを新規な記録媒体に複写可能な情報処理装置において、前記受信データが著作権により保護されたデータであるか否かを識別するための著作権保護識別手段と、前記記録媒体の信頼度を判定するための信頼度判定手段とを備え、前記著作権保護識別手段において著作権により保護されていると識別されたデータに対して、前記暗号化手段により暗号化を行う際に、前記信頼度判定手段において前記記録媒体の信頼度が高いと判定された場合には、前記記録媒体の固有情報に基づいて暗号鍵を生成して暗号化を行うとともに、前記信頼度判定手段において前記記録媒体の信頼度が低いと判定された場合には、当該情報処理装置の固有情報に基づいて暗号鍵を生成して暗号化を行うことにより、著作権を保護することを特徴とするものである。

【0015】また、前記情報処理装置において、前記記録媒体に記録されたデータに対して用いられている暗号鍵の種類を識別するための暗号鍵識別手段を備えることが可能である。

【0016】また、前記情報処理装置において、前記記録媒体に対してデータを暗号化して記録する際に、当該記録媒体において前記暗号鍵の種類が混在しないようにすることが可能である。

【0017】さらに、本発明に係る情報処理装置は、データを受信するための受信手段と、該受信手段により受信した受信データが著作権により保護されたデータであるか否かを識別するための著作権保護識別手段と、前記受信データから著作権情報を検出して著作権管理情報を生成するための著作権情報管理手段と、前記受信データを暗号化するための暗号化手段と、該暗号化手段により暗号化した前記受信データを交換可能な記録媒体に記録するための記憶手段とを備え、前記記録媒体に記録された受信データを新規な記録媒体に複写可能な情報処理装

置において、当該情報処理装置の固有情報と、前記受信データの著作権情報と、前記著作権情報管理手段で生成した著作権管理情報とに基づいて暗号鍵を生成するための暗号鍵作成手段を備え、前記受信データに対して、前記暗号鍵作成手段で作成した暗号鍵を用いて暗号化を行い暗号化済受信データを生成し、該暗号化済受信データを前記記録媒体に記録することを特徴とするものである。

【0018】また、前記情報処理装置において、前記受信データの著作権情報が許可した範囲において、前記暗号化済受信データと、該暗号化済受信データを複合化するための暗号鍵を送出し、新規な記録媒体に複製可能とすることができる。

【0019】

【発明の実施の形態】以下、図面に基づいて、本発明に係る情報処理装置の一実施形態を説明する。図1は、本発明の一実施形態に係る情報処理装置の概略構成を示すブロック図である。本発明の一実施形態に係る情報処理装置1は、図1に示すように、交換可能な記録媒体2に対してデータを記録するとともに、この記録媒体2に記録されたデータを新規な記録媒体に複写することが可能な装置である。

【0020】この情報処理装置1は、データの送受信を行うための通信機能部3と、受信したデータが著作権保護データか否かを識別するための著作権保護識別部4と、データを暗号化するためのデータ暗号部5と、データを暗号化する際に使用する暗号鍵を生成するための暗号鍵生成部6と、記録媒体2あるいは情報処理装置1の固有情報を取得して出力するための固有情報取得・出力部7と、記録媒体2の信頼度を判定するための信頼度判定部8と、記録媒体2に記録されたデータに対して使用されている暗号鍵の種類を識別するための暗号鍵識別判定部9と、記録媒体2に記録されたデータを復号化するための暗号化データ復号部10と、復号化したデータを外部に出力するための表示・外部出力インターフェイス部11とを備えている。また、記録媒体2には、記録されたデータに使用されている暗号鍵を認識するための暗号鍵認識手段12が付加されている。

【0021】この情報処理装置1において、通信機能部3で受信したデータは、著作権保護識別部4において著作権保護が行われている著作物か否かが識別される。本実施形態に係る情報処理装置1では、データの種類(DVDあるいはDVC等)毎に定められている規格に基づいて、著作権保護の識別を行なう。なお、本実施形態に係る情報処理装置1では、著作権保護が行われていない著作物の暗号化(鍵)については特定しないことを前提としているため、著作権保護が行われているデータの暗号化のみについて説明する。

【0022】次に、図2に示すフローチャートに基づいて、本実施形態に係る情報処理装置1の動作を説明す

る。本実施形態に係る情報処理装置1では、通信機能部3により、通信網を介してデータを受信し、著作権保護識別部4により、著作権保護が行われているデータか否かを識別する。そして、著作権保護が行われているデータである場合には、図2に示すように、暗号鍵識別判定部9により、交換可能な記録媒体2に記録されている暗号鍵の有無を判断する(S0a)。

【0023】ここで、暗号鍵が無い場合には、信頼度判定部8により、記録媒体2から読み出した信頼度に関するデータを収集して信頼度の判定(S0b)を行う。一方、暗号鍵がある場合には、当該暗号鍵が記録媒体2の固有情報か否かを判別し(S1)、記録媒体2の固有情報である場合には、信頼度判定部8により、記録媒体2から読み出した信頼度に関するデータを収集して信頼度の判定(S0b)を行う。

【0024】信頼度に関するデータは、記録媒体2の種類により異なるが、例えば、記録媒体2にアクセスされた回数を初期情報エリアに書き込んでおく。そして、アクセス累積回数情報を読み出し、予め情報処理装置1のROM等に設定されたアクセス回数の規定値と比較することにより信頼度を判定する。また、例えば、所定のタイミングで、記録媒体2の特定の空きエリアに信頼度測定用信号を記録するとともに、この信頼度測定用信号を再生し、再生時のエラー値と予め情報処理装置1のROMに設定されたエラー値とを比較することにより信頼度を判定する方法がある。記録媒体2としてEEPROMを使用した場合には、およその書き換え寿命は数十万回程度と言われている。

【0025】信頼度の判定処理(S0b)において記録媒体2の信頼度が設定値以上(信頼度が高い)であると判定された場合には、固有情報取得・出力部7により、記録媒体2の固有情報を取得する(S2)。また、記録媒体2の信頼度が設定値以下(信頼度が低い)であると判定された場合、および暗号鍵の判別処理(S1)において記録媒体2の固有情報でないと判別された場合には、固有情報取得・出力部7により、情報処理装置1の固有情報を取得する(S3)。

【0026】記録媒体2の固有情報とは、記録媒体2毎に異なる情報(例えば製造番号等の連続する番号など)のことであり、情報処理装置1の固有情報とは、情報処理装置1毎に異なる情報(例えばROM格納された製造番号やCPU毎に割り振られた識別番号など)のことである。また、記録媒体2の固有情報は、予め記録媒体2の初期情報として格納されているものとし、情報処理装置1の固有情報は、予め情報処理装置1内のROMに格納されているものとする。

【0027】暗号鍵生成部6では、固有情報取得・出力部7で取得した各固有情報に基づいてそれぞれ暗号鍵を生成する(S4、S5)。続いて、データ暗号化部5により、暗号鍵生成部6で生成した暗号鍵に基づいて、受

信したデータを暗号化する（S6）。暗号化されたデータは、記録媒体2に記録保存されると同時に、暗号鍵認識手段12により、記録媒体2の固有情報に基づいて生成した暗号鍵か（S7）、情報処理装置1の固有情報に基づいて生成した暗号鍵か（S8）が判別される。

【0028】暗号鍵認識手段12による暗号鍵の認識方法は、前記何れかの暗号鍵を、データとして記録媒体2に関連付けして記録する方法を用いることができる。また、前記何れかの暗号鍵を印刷したり、凹凸でマーキングすることにより、記録媒体2に物理的に認識ができる方法を用いることもできる。

【0029】また、既に当該情報処理装置1を用いてデータが記録されている記録媒体2が、情報処理装置1に装着された場合には、記録媒体2の暗号鍵認識手段12において暗号鍵を判別することができるので、ステップ1（S1）で判別した暗号鍵が情報処理装置1の固有情報に基づいて生成した暗号鍵であれば、情報処理装置1の固有情報に基づいて生成した暗号鍵により受信データの暗号化を行う。このように、暗号鍵認識手段12による判別（S1）を、記録媒体2の信頼性の判定（S0b）よりも優先させることにより、記録媒体2に対する暗号鍵方式の混在を防止することができる。

【0030】また、ステップ1（S1）で判別した暗号鍵が記録媒体2の固有情報に基づいて生成した暗号鍵であった場合には、記録媒体2の信頼度判定（S0b）を行なう。そして、信頼度が低いと判定された場合には、記録媒体2を交換して、新規な記録媒体2によりデータの記録を行うように警告を発する。ここで、ユーザが記録媒体2の交換を拒否（信頼性が低いままの記録媒体2でデータを追加する）した場合には、記録媒体2の固有情報に基づいて生成した暗号鍵によりデータの暗号化を行なう。

【0031】また、記録媒体2の信頼度判定処理（S0b）において、情報処理装置1の固有情報に基づいて暗号鍵を生成する場合の回数の上限値は、前記受信データの著作権保護データ内における複写回数の指定により制限してもよい。

【0032】記録媒体2に保存された暗号化データは、記録媒体2の暗号鍵認識手段12により認識され、暗号鍵識別判定部9により暗号鍵の種類が判定されて暗号鍵が得られる。そして、暗号化データ復号部10により、暗号鍵と記録媒体2に記録されている暗号化データに基づいてデータが復号される。復号されたデータは、表示・外部出力インターフェイス部11に入力され、夫々の用途に使用することができる。

【0033】次に、本発明に係る情報処理装置の他の実施形態を説明する。

【0034】図3は、本発明の他の実施形態に係る情報処理装置の概略構成を示すブロック図である。本発明の他の実施形態に係る情報処理装置21は、図3に示すよ

うに、データの送受信を行なうための通信機能部23と、受信したデータが著作権保護データか否かを識別するための著作権保護識別部24と、データを暗号化するためのデータ暗号部25と、データを暗号化際に使用する暗号鍵を生成するための暗号鍵A生成部26および暗号鍵B生成部27と、情報処理装置21の固有情報を取得して出力するための固有情報取得・出力部28と、受信データから取得される著作権情報を管理するための著作権情報管理部29と、記録媒体22に記録されたデータを復号化するための暗号化データ復号部30と、復号化したデータを外部に出力するための表示・外部出力インターフェイス部31とを備えている。また、記録媒体22には、記録されたデータに使用されている暗号鍵情報を管理するための鍵情報管理部32が付加されている。情報処理装置21の固有情報とは、情報処理装置21毎に異なる情報、例えばROM内部に格納されている製造番号などのことである。

【0035】この情報処理装置21において、通信機能部23で受信したデータは、著作権保護識別部24において著作権保護の対象データか否かが識別される。本実施形態に係る情報処理装置21では、データの種類（DVDやDVC等）毎に定められている規格に基づいて、著作権保護の識別を行なう。

【0036】次に、図4に示すフローチャートに基づいて、本実施形態に係る情報処理装置21の動作を説明する。本実施形態に係る情報処理装置21では、通信機能部23により、通信網を介してデータを受信し、著作権保護識別部24により、著作権保護の対象データか否かを識別する。そして、著作権保護のデータである場合には、図4に示すように、著作権者からデータの複製が許可されているか否かの情報を取得して当該制限内容を判断する（S11）。

【0037】ここで、データの複製が許可されていない場合には、複製許可回数と複製許可回数残回数をともにゼロとして（S12）、複製を禁止する（S12）。そして、複製許可回数を取得するとともに（S13）、複製許可残回数を取得し（S14）、取得した複製許可回数および複製許可残回数に基づいて、暗号鍵A生成部26により暗号鍵Aを生成する（S15）。したがって、暗号鍵Aには、著作権情報に基づく複製制限情報が含まれることとなる。

【0038】また、固有情報取得・出力部28から装置固有情報を取得し（S16）、この装置固有情報および複製許可回数に基づいて、暗号鍵B生成部27により暗号鍵Bを生成する（S17）。したがって、暗号鍵Bには、装置固有情報と複製可否情報が含まれることとなる。続いて、データ暗号部25において、生成された暗号鍵Aと暗号鍵Bとに基づいて、受信したデータを暗号化する（S18）。暗号化されたデータは、記録媒体22に保存され（S19）、暗号化に使用した暗号鍵Aと

暗号鍵Bの情報は、鍵情報管理部32で管理される。

【0039】記録媒体22に記録された暗号化データは、鍵情報管理部32で管理される情報に基づいて、暗号化データ復号部30により、各暗号鍵と記録媒体22に記録されている暗号化データから復号され、表示・外部出力インターフェイス部31へ送られ、表示あるいは出力される。

【0040】

【発明の効果】本発明に係る情報処理装置によれば、著作権により保護されたデータが記録されている記録媒体の信頼度判定を行い、記録媒体の信頼度が高い場合には記録媒体の固有情報に基づいて暗号鍵を生成し、記録媒体の信頼度が低くなると情報処理装置の固有情報に基づいて暗号鍵が生成される。したがって、記録媒体の信頼度が低くなった場合には、新規な記録媒体と入れ替えて複写を行うことが可能になり、重要なデータを失うおそれなくなる。

【0041】また、新規な記録媒体に複写された複写データから暗号鍵を生成する場合には、この新規な記録媒体の信頼性判定を行う（当然信頼性が高い）ので、当該新規な記録媒体の固有情報に基づいて暗号鍵が生成され、著作権が保護される。

【0042】また、本発明に係る情報処理装置によれば、記録媒体に対して記録されたデータの暗号鍵方式を識別することができるので、使用者が暗号鍵の種類を判断して情報処理装置に入力する必要はなく、情報処理装置において自動的に暗号鍵の種類が認識される。

【0043】また、本発明に係る情報処理装置によれば、記録媒体に記録されたデータに対して暗号鍵の種類が混在することがないので、データの管理が容易となる。

【0044】また、本発明に係る情報処理装置によれば、情報処理装置の固有情報と、受信データの著作権情報と、著作権情報管理手段で生成した著作権管理情報とに基づいて暗号鍵が生成される。したがって、暗号鍵を

生成するため著作権保護の対象となる暗号化データを複製しようとした場合に、暗号鍵が保持する複製制限情報および複製可否情報に基づいた複製管理が可能となる。さらに、暗号鍵は装置固有情報を保持しているので、ユーザーが他の情報処理装置へのデータ移動を望む場合であっても、著作権保持者がその行為を許可しているのであれば、装置固有情報を参照しない状態における一過性の複製が可能となる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る情報処理装置の概略構成を示すブロック図である。

【図2】本発明の一実施形態に係る情報処理装置の動作を示すフローチャートである。

【図3】本発明の他の実施形態に係る情報処理装置の概略構成を示すブロック図である。

【図4】本発明の他の実施形態に係る情報処理装置の動作を示すフローチャートである。

【符号の説明】

- 1、21 情報処理装置
- 2、22 記録媒体
- 3、23 通信機能部
- 4、24 著作権保護識別部
- 5、25 データ暗号部
- 6 暗号鍵生成部
- 7 固有情報取得・出力部
- 8 信頼度判定部
- 9 暗号鍵識別判定部
- 10、30 暗号化データ復号部
- 11、31 表示・外部出力インターフェイス部
- 12 暗号鍵認識手段
- 26 暗号鍵A生成部
- 27 暗号鍵B生成部
- 28 固有情報取得・出力部
- 29 著作権情報管理部
- 32 鍵情報管理部

